
RECOMMENDATIONS
FOR THE
HACKTIVIST COMMUNITY

- - -

Released on this day of November the 5th, 2014

Penned by The Humble Observer

Statement of Purpose

I have been observing the hacker and hacktivist communities, at times very closely, for many years. The exact definition of "hacker" and "hacktivist" varies from author to author, so I shall make my interpretation of these words very clear. Let us define a "hacker" as someone who utilizes their knowledge of computers and of computer networks to make money via illegitimate means. Let us define a "hacktivist" as someone who utilizes their knowledge of computers and of computer networks to do justice when justice is not done by the state. I have found that these two communities are inextricably linked, yet remain completely separate entities. Many hackers double as hacktivists in their spare time, although most hacktivists do not fancy themselves hackers.

Although hackers turned hacktivists have the very best of intentions, and their input and expertise is of great value to the hacktivist community, they have inadvertently suppressed the potential of the very community they are trying to aid. The get-in-get-the-goods-get-out methodology of the stolen credit card driven hacker community that has been transferred to the hacktivist community via ideological osmosis has tragically affixed blinders to it. It has caused the hacktivist community to think linearly and strive to do nothing more than to blindly infiltrate target organizations and immediately leak whatever data they happen to stumble across. This must change. Stealing and leaking data makes a point, but it is sometimes necessary to do more than just make a point, to inflict real, measurable damage. In certain, extreme cases an organization's

disregard for human rights warrants its immediate and complete obliteration.

In this essay, I will discuss a multitude of ideological, operational, and technical changes that ought to be made to the hacktivist community. These proposed changes have been derived from my personal observations. Some will find the ideas contained within this document to be the product of common sense. I have found these people to be few in number. If the community accepts my suggestions it will not only become more effective, but the risks associated with participating in it will be drastically lowered. My intent in writing this is not to aid criminals, but rather to aid people who wish to do battle with governments and corporations that have become criminals. If freedom is to remain on this earth, its people must be willing and able to take arms to defend it, both physical and digital.

Personal Security

Sound operational security is the foundation from which all effective cyber-offensives are launched. You should, at all times, put your own, personal security above the success of your operations and interests. The security precautions taken by most hacktivists I have met are mediocre at best, and needlessly so. Maintaining sound personal security is by no means difficult. It requires much caution but very little skill. I have devised a series of security precautions that hacktivists should take and divided them up into six main categories: environmental, hardware, software, mental, pattern related, and archaeological. We shall examine each individually.

(1) Environmental:

There are but two places you can work: at home or in public. Some people insist that working at home is best and others insist that working in public is best. The proper working environment debate has been raging on in the hacker community for quite some time now, and has great relevance to the hacktivist community, as most governments view hackers and hacktivists as one in the same. Proponents of the "work in public" argument claim that by always working at a different public location, you significantly lower your chances of being apprehended. They argue that even if the authorities are able to trace many of the cyber-attacks you took part in back to the public places where you took part in them from, that does not bring them any closer to finding you. Most retail stores and coffee shops do not keep surveillance footage for more than a year at the most, and even if the authorities are able to get a photo of you from some security camera, that does not necessarily lead them directly to your front door, especially if you wore a hoody the entire time you were working and the camera never got a clear shot of your face. On the other hand, proponents of the "work at home" argument argue that the risk of being seen and reported, or merely recorded while working in a public place far outweighs the benefits of the significantly large increase in anonymity that working in public provides. Both sides have legitimate points, and I urge you to consider

both of them.

If you decide to work in public, the number one threat you face is other people. Numerous large criminal investigations have been solved using the observations of average everyday citizens who just happened to remember seeing something suspicious. If people sense that you are trying to hide something, they will watch you more closely than they would otherwise. It is important to always "keep your cool" as the old saying goes. Always try to sit in such a way that your screen is facing away from the majority of the people in the room you are sitting in. Corners are your friend. Try to blend in with the crowd. Dress in plain cloths. Draw no attention. If you are in a coffee shop, sip some coffee while you work. If you are in a burger joint, buy a burger. If you are in a library or book store, set a few books beside your laptop. Also, be very aware of security cameras, both inside the establishment you are working in as well as on the street near it. Being captured on film is alright as long as the camera can not see what is on your screen. Some store cameras are watched by actual people who will undoubtedly report you if they find out what you are doing. More and more governments are starting to place very high quality CCTV cameras on their streets to monitor their citizens, and these devices can be a problem if they are peering over your shoulder through a window you are sitting beside. When working in public, it is possible that you may have to confront a law enforcement officer face to face. Law enforcement officers can smell uneasiness from a mile away, and if you look like you are up to no good it is possible that a cop will come and talk to you. Always have some sort of cover story made up before you leave home to explain why you are where you are. If you are forced to confront a law enforcement officer you should be able to talk your way out of the situation.

If you decide to work at home, the number one threat you face is your own ego. Just because you are at home does not mean that your working environment is secure. Be aware of windows in close proximity to your computer as well as your security-illiterate or gossipy family members. Security issues in relation to network configuration begin to come into play when you work at home. If your computer were to somehow get compromised while you are working at home, perhaps by your government, it would be nearly impossible for the person or group of people rummaging around inside of your system to get your actual IP address (provided that you adhere to the software security guidelines that we will discuss later). However, if your wi-fi password (or the name of your printer, or the name of another computer on the network) contains your actual last name and part of your address, tracking you down becomes very easy. A lot of people name their network devices and structure their network passwords in this way.

It is also possible that if an attacker that has infiltrated your computer notices other machines on your network they can pivot to them (infect them with malware using your computer as a spring board of sorts) and use them to get your IP address. A lot of Internet enabled household devices have cameras on them (your smart TV, your Xbox, and your high tech baby monitor to name a few) and said cameras can potentially be leveraged against you. It is in your best interest to not have any other machines running on your home network while you are working. Also, change your wi-fi password every once in awhile and make

sure that the password on the administrative interface of your router is something other than the out-of-the-box default. If your computer gets compromised, logging into your router using username "admin" and password "admin" is elementary for a moderately skilled attacker. Most modern routers list their WAN IP address on their control panels.

Regardless of where you decide to work, be aware of mirrors and glass picture frames near your workplace. In the right light, both of these items have the potential to reflect crystal clear images of your screen to onlookers across the room. In addition to this, understand that modern cell phones are your worst enemy. Not only are they always going to be the weakest link in your security setup, but if they are somehow compromised they are equipped with a camera and microphone. Recent studies suggest that it is possible for smart phones to listen to the high pitched noise your CPU makes and deduce your PGP private key. Furthermore, the metadata collected by your phone coupled with pattern analysis techniques could potentially allow your government to link your real life and online personas together after some time. We will discuss this in depth later. Leave your phones at home and if possible keep all phones, yours or otherwise, far away from your computer. Other portable devices such as iPods and tablets potentially pose the same risk that phones do and should be treated the same.

(2) Hardware:

Modern computers come equipped with microphones, speakers (which can be used as microphones under the right circumstances), and cameras. All of these features can potentially be leveraged to identify you if your computer is compromised. To mitigate these risks, these features should be physically removed. Your computer's microphone and speakers should be ripped out of it, but you should not rip out your web cam, as it will alter the outward appearance of your computer and potentially draw attention to you. Instead, open your computer's screen and snip the wires that connect to your web cam. Wrap the ends of the wires in electrical tape so sparks do not jump in between them. If you must listen to an audio file while working, use headphones. Only keep your headphones plugged into your computer when you are using them. The computer you use for your hacktivist activities also should not contain a hard drive, as they are unnecessary for our purposes.

(3) Software:

Always use a TOR enabled Linux live system when working. At the present moment, Tails (The Amnesiac Incognito Live System) is by far the best live distribution for your purposes. You can read more about TOR at www.torproject.org and you can read more about acquiring, setting up, and using Tails at tails.boum.org. The Tails operating system lives on a USB flash drive. Every time you start up your computer, you must first insert your Tails flash drive into it. The Tails website will guide you through making said flash drive. Tails will automatically direct all of your outgoing traffic into the TOR network in an effort to hide your IP address. If you use Tails you will be completely anonymous and be able to work with impunity provided that:

- * You keep your Tails USB up to date. New versions of the Tails operating system are released every few months.
- * You do not login into your “real world” accounts while using Tails. Do not check your Twitter feed while you are working.
- * You do not use Tails to create an account with an alias that you have used before. If you have been “Opwn” for the past seven years, now is a good time to stop being Opwn.
- * You do not alter Tails' default security settings. They are the way they are for a reason.
- * You do not use Tails to create an online account with a password that you have used before. Doing this only makes deanonymizing you easier.
- * You do not install and use random packages that “look cool”; they could be miscellaneous. Only use packages and scripts that you trust. Tails is not bullet proof.
- * If you decide to set a sudo password when starting up Tails, make sure that it is very strong.
- * You stay conscious of metadata analysis techniques. We will discuss these later.
- * You switch exit nodes every ten to fifteen minutes. This can be done by double clicking the little green onion in the upper right hand corner of your Tails desktop and hitting the “Use a New Identity” button.
- * You follow the communication guidelines laid out later in this document.

More information can be found on the Tails warning page: <https://tails.boum.org/doc/about/warning/index.en.html>. Be aware that it is very easy for your ISP (which is probably working closely with your government) to tell that you are using both TOR and Tails. It is probably in your best interest to use something called “TOR bridge mode”. You can read more about how to configure Tails to use TOR bridges here: https://tails.boum.org/doc/first_steps/startup_options/bridge_mode/index.en.html.

Tails is unique in that it has a special feature that wipes your computer's memory before it shuts down. This is done in order to mitigate risks associated with the dreaded “cold boot attack” (a forensics method in which a suspects RAM is ripped out of his or her computer and then thrown into a vat of liquid nitrogen to preserve its contents for later analysis). This feature is also triggered if you pull your Tails flash drive out of your computer while you are working. If while you are working you ever feel that the authorities are about to move in on you, even if you have a seemingly irrational gut feeling, yank your Tails flash drive out of your computer. Tails also has a feature that

allows it to disguise itself as a Windows desktop. Using this feature in public will reduce your risk of capture significantly.

(4) Mental:

A skilled attacker is well disciplined and knows that he must keep his actions and skills a secret in order to remain safe from harm. Do not flaunt the fact that you are dissatisfied with your government, a foreign government, or a particular corporation. Do not attend protests. Do not publicly advertise the fact that you have an above average aptitude for computer security offensive or otherwise. And whatever you do, do not tell anyone, even someone you think you can trust, that you are planning to launch an organized cyber-attack on any organization, big or small. If you draw attention to yourself no amount of security precautions will keep you safe. Keep your "real" life mentally isolated from your "hacktivist" life. One lapse in operational security could end you.

Be alert and focused. Remain mentally strong. Come to terms with the illegality of your actions and what will happen to you if you are apprehended. As a wise man once said, "A warrior considers himself already dead, so there is nothing to lose. The worst has already happened to him, therefore he's clear and calm; judging him by his acts or by his words, one would never suspect that he has witnessed everything." It is perfectly acceptable to be paranoid, but do not let that paranoia consume you and slow your work. Even if you are extremely cautious and follow this document's advice to the letter, you still may be hunted down and incarcerated, tortured, or killed. Some countries do not take kindly to hacktivists. It is best that you be honest with yourself from the beginning. In order to operate effectively you must be able to think clearly and see the world as it actually is.

(5) Pattern Related:

When your online persona is active your real life persona ceases to exist, and an observant adversary can use this to their advantage. If your ISP, bank, and mobile phone provider are "cooperating" with your government and allowing them to browse through all of their records (a fair assumption in this day and age) then, eventually, they will be able to deduce your real identity by comparing everyone's data to information about your online persona. If the government looks back on all of the records they have collected in the past year and notice that you never make a credit card purchase, watch Netflix, go on your Facebook, Google, or Twitter account, or change your physical location while 1337Hax0r64 is online on some anti-government forum on the deep web, they will assume that you are 1337Hax0r64. Even information about your home network's bandwidth usage can give away your real identity.

Luckily, performing the type of metadata analysis attack described above takes time, usually many months. It is very important that you change aliases often, preferably every three or four months. Shed your old names like a snake sheds its skin. When you do change your online name, make sure your new identity can not be tied back to your old one.

DO NOT not launch cyber-attacks from your own computer. Launch attacks only from hacked servers, servers purchased with washed bitcoins, or free shell accounts. Certain types of cyber-attacks produce a large amount of traffic over a short amount of time. If the bandwidth usage of your home network spikes at the same instant that a government or corporate server is attacked, the time it takes to deanonymize you is reduced significantly. This is especially true if you launch multiple attacks on multiple occasions. Launching attacks in this way can be mentally exhausting. Configuring a new attack server with your tool set every time your old attack server is banned (an inevitable occurrence) can be a tedious task indeed. I personally recommend creating a bash script to automatically install your favorite tools to make this transition process easier. Most hackers and offensive security professionals use under thirty non-standard tools to do their job, so configuring a new server with everything you need should not take very long if you know what you are doing. Consider equipping your server with TOR and a VNC server (for tools that require GUIs such as most popular intercepting proxies) as well.

(6) Archaeological:

You must insure that there is no forensics evidence of your actions, digital or otherwise. If the government breaks into your house and rummages through your things, they should find nothing interesting. Make sure that you never make any physical notes pertaining to your hacktivist activities. Never keep any computer files pertaining to your hacktivist activities in your home. Keep all of your compromising files, notes, scripts, and unusual attack tools (the ones that can not be installed with apt-get or the like), and stolen information in the cloud. It is recommended that you keep all of your files backed up on multiple free cloud storage providers so that in the event that one of the providers bans your account you still have all of your data. Do not name your cloud accounts in such a way that they can be connected back to your online persona. Never, under any circumstances, mention the names or locations of your cloud accounts to the people you work with. Always hit the "Use New Identity" button on your TOR control panel after accessing your cloud storage solutions. Every time you shed your old alias, shed your old cloud accounts.

Security of Communications

The majority of hacktivists I have met communicate via public IRC. Using IRC is fine for meeting other hacktivists, but as soon as you muster a team of other hacktivists who wish to attack the same target as you, move to another more secure form of communication. Some means of communication are more secure than others, but completely secure communication does not exist. The following guidelines are meant to work in conjunction with the personal security guidelines that were discussed in the previous section. If proper personal security measures are implemented effectively, compromised communication will result in operational failure at worst and not complete deanonymization. Since operational failure may very well set you and your cause back several months,

it is in your best interest to attempt to communicate securely:

- * Remember that any of the people you meet on the clearnet, deep web, or public IRC channels who claim to be on your side could actually be government agents trying to sabotage your operations.
- * If possible, communicate mainly via privacy friendly email accounts (not Gmail, Yahoo, AT&T, etc.) and encrypt all of your messages with PGP. When a cyber-attack is being carried out it is often necessary to be able to communicate with your accomplices instantaneously. Since encrypting, sending, receiving, and decrypting messages by hand takes time, using PGP in time sensitive situations like this is not feasible. If you have to confer in an IM environment, use a program like TorChat that uses its own form of asymmetric encryption to send and receive messages instantly.
- * Use strong passwords for all of your online accounts. The best way to make a strong password is to pick eight or nine random words and string them together. Passwords like this are easy to remember but hard to guess.
- * Never give away any personal information (such as country, interests, hobbies, health, etc.) or give insight into your feelings or emotions. Your fellow hacktivists are not your friends and should never be talked to as such. Giving away this sort of information will make tracking you easier.
- * When you receive messages, do not retain them, even if they are encrypted. Read them, make note of any hard to remember details (like long server passwords for example), and then delete them. Having a mile long digital paper trail can not lead to anything good. In some cases deleted messages on email servers can be recovered via computer forensics, but deleting messages quickly may reduce the odds that they can be.
- * When typing messages, do so in a word processor on your computer. Never write your message inside of a communication program (such as an online email client, forum PM box, etc.). People have been known to accidentally send unencrypted messages before. The effects of such an error can be devastating.
- * If you find yourself writing large swaths of text intended for public release (like essays or manifestos) use a tool like Anonymouth to obscure your writing style. Your writing style is as unique as a finger print and can be used to identify you.
- * Never, under any circumstances, execute a file on your computer or on your server that has been given to you by a fellow hacktivist. You should never run into a situation where doing this is necessary.
- * Do not disclose information about your involvement in previous

hacktivist operations to people who were not also part of the same operation.

- * If one of the people that you are working with gets captured, assume that the people who have captured them know everything that they do.

Philosophy of Attacking

The hacktivist community, like every community, has its own unique set of philosophical musings, taboos, and dogmas. While I do not advocate the severe alteration of the principles and philosophies on which the community was built, I do wish to point out a number of flaws in certain aspects of their composition. These flaws serve only to hold back the community and should be openly discussed.

(1) When hacktivists target an organization, their goal is more often than not to force said organization to stop functioning permanently, or at least for the longest time possible, in an effort to stall unjust actions from being carried out or to seek retribution for unjust actions done in the past. Leaking databases, DoXing influential individuals, defacing websites, and launching massive DDoS campaigns, four of the modern hacktivist community's favorite activities, accomplish this goal – to an extent. Infiltrating a target organization and sowing discord within its ranks is magnitudes more effective than leaking credit card numbers or putting a CEO's social security number on Pastebin, yet it is rarely, if ever, considered to be a viable course of action. Subtly and silently fostering suspicion and distrust inside of your target will have a longer lasting impact than simply pointing out that its security policy has some weak points.

(2) Hacktivists crave publicity, yet they are the most effective when they operate undetected. Stay hidden. Although it may seem tempting at times, do not destroy large amounts of information on your target's computers or servers. Doing so will announce your arrival inside of your target's network rather loudly. Flashy, public displays of power have no place in the hacktivist community. Just because you are hiding behind TOR does not mean that you should not make an effort to cover your tracks. Conceal your attack not to mask your identity, but to convince your target that no attack was carried out in the first place.

(3) Once your hacktivist collective has decided to attack an organization, strike fast and strike hard. Overwhelm your target. A well disciplined and well organized team of attackers can penetrate most networks within a few hours. Far too often I have seen hacktivist collectives declare all out war on someone and then attack them slowly and gain entry into their network days, sometimes even weeks later. By attacking slowly, you give your target time to react and strengthen their defenses. Detecting an attack from a large hacktivist collective is a trivial task, but as history has shown detecting the presence

of one inside of a network, especially a large network, can be tricky.

(4) Cyber-attacks seldom go as planned. If you are attempting to do anything that involves the coordination of more than two people, keep this in mind. It is not uncommon for tools to stop working in the middle of an attack. It is not uncommon for reverse shells to die unexpectedly. It is not uncommon for seemingly simple actions to take hours to perform. You must be ready to think on your feet and quickly adjust your attack plan to accommodate the ever changing conditions within the network you are attacking. Predefined contingency plans are mostly useless.

(5) Remember that no system is impenetrable. On more than one occasion I have seen hacktivists give up on trying to infiltrate a target network because their Nessus scan did not yield any useful results. As a hacktivist, you are not bound by the typical constraints of a pentester. If you can not successfully attack a website, try attacking its hosting provider. Try attacking the administrator's email account. Try going after random social accounts belonging to the administrator's family. Try planting iframes in websites you suspect the administrator frequents in an effort to infect him. If you cause extensive collateral damage, who cares? It is not your problem. Sometimes the ends justify the means. Be creative.

(6) Many hacktivists possess unrealistic, self-constructed mental images of the ideal cyber-attack. In the majority of these movie-induced delusions, the ideal attack utilizes numerous 0days, an arsenal of home made tools, and highly advanced, unimaginably complex network intrusion techniques. In reality, this type of thinking is incredibly dangerous and causes some hacktivists to attempt to perform convoluted, elaborate attacks to gain the respect of their peers. When breaking into highly secured networks, such attacks only draw unnecessary attention. The best attacks are the ones that work. They are usually simple and take little time to execute. Using sqlmap to spawn a shell on your target's server by exploiting a flaw in their website's search feature is a viable if not ideal attack. It allows you to access the inside of your target's network. Exploiting a vulnerable FTP daemon on one of your target's servers using public exploit code is a viable if not ideal attack. It allows you to access the inside of your target's network. Using Metasploit in conjunction with a fresh Gmail account to launch a phishing campaign against your target's employees is a viable if not ideal attack. It allows you to access the inside of your target's network. The media hates it when hacktivists use open source software to do their work. Whenever a hacker or hacktivist is arrested for doing something that involved using "someone else's" tools, they are publicly shammed. "Anyone could have done that" they say. "He's just an unskilled script kiddie" they say. Claiming that someone is less of a hacker solely because they partially depend on someone else's code borders on absurd. It amounts to claiming that Picasso is a bad artist because he did not carve his own brushes, synthesize his own paints, and weave his own canvas. Do not shy away from using open source tools and publicly available information to accomplish your goals. Hacking is an art, and nmap is your brush.

Organization and Formation

Most of the hacker and hacktivist groups I have observed are unorganized and undisciplined. They claim to perform actions as a collective, yet when it comes time to actually launch an attack they attempt to infiltrate their targets as individuals, each member launching attacks of their own without making the faintest attempt to coordinate their actions with others. Here I shall describe a schema that could be easily adopted by any hacktivist collective to allow it to facilitate highly coordinated attacks involving large numbers of attackers with great ease. It will be presented as a series of steps.

Step One: Organize yourselves into multiple small groups. These groups shall be referred to as strike teams. The ideal strike team is composed of three parts: attack specialists, two parts social engineering specialists. Attack specialists should at least be able to identify and competently exploit potential vulnerabilities in websites and be able to exploit vulnerable or misconfigured services. Social engineering specialists should have at least some real world experience before participating in a strike team. Attack specialists should only concern themselves with launching attacks and social engineering specialists should only concern themselves with social engineering. Well-defined roles are the key to a strike team's success. This configuration will often create an abundance of social engineering specialists, and that is perfectly acceptable. Having the capability to immediately launch multiple well planned social engineering campaigns is crucial. The size of a strike team will be determined by the skill of its members. Highly skilled individuals should work in very small strike teams (five member teams are acceptable) whereas unskilled individuals should work in larger strike teams (up to a few dozen). The organization of strike teams should be coordinated as a collective. No one person should be given the authority to sort people themselves. Strike teams should function as "sub collectives" and be autonomous. Hacktivist collectives are composed of people around the world, most of whom can not be online all the time. This means that all strike teams should set themselves up knowing that their members will pop on and offline and that it is possible new members will have to be annexed at a later time.

Step Two: Within each strike team, agree upon a stratagem; a broad, realistic, nonspecific plan of action that aims to accomplish one, very specific goal. Strike teams should only execute one stratagem at a time. Multiple strike teams within the same hacktivist collective can execute different stratagems at the same time in an effort to accomplish some sort of final goal (perhaps to destabilize an organization or to acquire trade secrets). The next section of this essay is devoted solely to exploring the concept of stratagems and how to best form and use them. Strike teams should be allowed to do what they want, but their initial stratagem should be approved by the collective so that no two strike teams attempt to do the same thing at the same time.

Step Three: As a strike team, map your target's attack surface. If multiple strike teams are all attacking the same network, they should share information very closely in this step. It is very possible that multiple strike teams

working together to accomplish the same goal could actually be attacking different networks, in which case mapping should be done within individual strike teams. Each member of a given strike team should attempt to map the target network themselves, and then members should compare information. It is very unlikely that anything will be overlooked by every single member of the team.

Step Four: Divide your target network up into manageable chunks and assign certain individuals within your team to each one of those chunks. Efficient division of labor is key to launching speedy attacks. Here is an example involving a network composed of four servers (two SQL servers, a DNS server, and a web server hosting a feature rich corporate site) and a strike team composed of six attack specialists and four social engineering specialists:

- * Have one attack specialist attack the SQL and DNS servers.
- * Have one attack specialist attack the website's multistage user registration mechanism and login mechanism.
- * Have one attack specialist attack the contact and session management mechanism.
- * Have one attack specialist attack any forms not assigned to other attack specialists as well as any other potentially exploitable scripts, pages, or mechanisms.
- * Have one attack specialist and two social engineering specialists attempt to launch some sort of phishing campaign against the company's employees.
- * Have one attack specialist and two social engineering specialists attempt to convince the company's hosting provider that they are the rightful owners of the company's four servers and have been locked out of their email account.

Step Five: Drill yourselves. This step is optional but highly recommended. Procure a server with a large amount of RAM and multiple processors. Have one member of your strike team set up a virtual network on it that, to the best of your knowledge, mimics the network you are planning to attack. This one team member should not participate in the drills themselves, and they should not give other team members details pertaining to the virtual network. If you are planning on attacking a large cooperation, set up the virtual network like a large cooperate network with a labyrinth of firewalls, routers, switches, and domain controllers. If you are planning on attacking a small cooperation or home business, set up your network accordingly. You should never have to visualize more than 12 workstations, even if your team is doing a complex pivoting exercise. As a group, attempt to break into your virtual network and execute your stratagem. The virtual network should be deliberately misconfigured so that there is a way for your team to infiltrate it and accomplish their simulated goal, but the misconfigurations should be extremely subtle. The team should have to work very hard to find them. Run multiple

drills. After each drill, the misconfigurations in the network, and potentially the layout of the network itself, should be altered to force your team to attack it in a different way or to exercise a different skill. The purpose of these drills are two fold. Firstly, they allow your team members to get accustomed to working together. Secondly, they will prepare your team for the day when they actually go up against your real target network.

Step Six: Execute your stratagem on your target network. Your strike team should attack methodically and silently. Every member should know what they need to do and how they need to do it. No mistakes should be made. Every tool you use should be well honed and function flawlessly. Not a second should be wasted. Use time to your advantage. Your target organization will be the most unprepared for an attack in the middle of the night when all of its IT staff are at home sound asleep. If your stratagem calls for being embedded in your target network for a long period of time, tread very lightly once you infiltrate it.

Interlocking Stratagems in Theory

In this section I will give multiple examples of stratagems that an actual strike team could make use of. You should combine multiple stratagems to accomplish your ultimate goal. Individual stratagems are like pieces of a jigsaw puzzle, and are intended to be pieced together. A strike team should execute multiple stratagems in succession, possibly in cooperation with other strike teams in an effort to accomplish a common goal. This section is not intended to be a play book. I encourage you to build off of my stratagems or, better yet, devise your own. Some stratagems are:

- (1) Collect information on individuals within the target organization. Mount a phishing campaign against the organization and gain access to as many workstations as possible. Once you have breached its network, do not pivot. Attempt to locate any useful information on the workstations you have compromised, and then remain in the network for as long as possible doing nothing more than idly gathering intelligence.
- (2) Take complete or partial control over the target organization's main means of communication (usually email). Review a few of their messages and learn how they are structured and formatted. Then, send a number of blatantly false messages to one or more members of the organization using the credentials of another member of the organization. Multiple false messages should be sent over some period of time. When members of the organization begin to receive false messages from their colleagues, distrust will begin to take root.
- (3) Take complete or partial control over the target organization's main means of communication (usually email). Review a few of their messages and learn how they are structured and formatted. Then, devise some way to intercept and inspect or modify messages in transit within the target organization

(essentially, perform a man in the middle attack). Every once in awhile, alter a message in a subtle but disruptive way. Perhaps change a date or a time so certain individuals do not arrive at their meetings on time or do not arrive at all. Once you have reason to believe that your modifications have taken their toll (i.e. the person you targeted missed their meeting), undo the changes you made to the message you intercepted so upon audit it appears as though the message was never tampered with. Doing this is usually hard to detect and will slowly cause the target organization to destabilize itself as tensions between individuals within it begin to rise and their employees begin to question their own sanity.

(4) Take complete or partial control over the target organization's main means of communication (usually email). Review a few of their messages and learn how they are structured and formatted. Use the credentials of a high ranking individual within the target organization to distribute a message that appears to be from them that claims a terrible tragedy has occurred that warrants an immediate, brash, resource intensive response from the rest of the organization. You will most likely not be able to pull this off more than once. This stratagem works especially well against militant groups with poorly defined command structures but has other applications as well.

(5) Once inside of the target organization's network, acquire a small amount of classified data intended for the eyes of high ranking personnel only. Strategically plant the data on the computer of one or more lower ranking individuals. Make it look like an espionage attempt. If many key individuals within the target organization are accused of trying to siphon out its secrets, it will be forced to suspend a large portion of its operations while an investigation is done.

(6) Use a DDoS attack to disrupt the target organization's communications for a short period of time when they are most in need of it. For a corporation, this could be during an important international Skype call. For a government, this could be immediately following a devastating attack from an insurgency group. Doing this will cause panic, which will make the target organization temporarily more susceptible to other kinds of attacks.

(7) Pose as a legitimate company selling legitimate software and befriend the target organization. Create a piece of software with a very hard to detect security flaw in it and sell it to them. The flaw could be as simple as a poorly implemented encryption library or as complex as an insecure multistage parsing algorithm. It must be incredibly subtle. So subtle that if it is detected you will be able to write it off as unintentional. It should be plausibly deniable. Once the target organization installs the vulnerable software on their machines, leverage it to perform targeted attacks on key individuals within it. Do not use it to infect entire subnets, as that will draw too much attention.

(8) Locate a small software provider your target organization already does business with and infiltrate their network by using other stratagems. Modify their source code slightly so that their software becomes vulnerable to remote attack. Do not modify just any code you come across, study the software

provider's development process and target code that has already been checked for bugs and is days away from being released to customers. When the target organization installs the latest version of software from the company that you have infiltrated, they will become vulnerable. Leverage this vulnerability to perform targeted attacks on key individuals within the target organization. Do not use it to infect entire subnets, as that will draw too much attention.

(9) Locate a small software provider your target organization already does business with and infiltrate their network by using other stratagems. Most software companies offer rewards to security researchers who find vulnerabilities in their products. Determine how reported vulnerabilities are managed by the company you have infiltrated and devise a way to monitor them in real time. As soon as a security researcher reports a major vulnerability in a product your target organization uses, use it to perform targeted attacks on key individuals within it. Do not use it to infect entire subnets, as that will draw too much attention.

(10) Using other stratagems, infiltrate the computers of a number of influential individuals within the target organization. Monitor their activity constantly and closely. If possible, listen to them through their computer's microphone. When you believe that one of them has left their computer, undo things they have just done. Delete the last sentence they wrote. Hit the back button on their web browser. Close the program they just opened. Over time, this will lead them to question their sanity.

(11) Using other stratagems, infiltrate the computers of a number of influential individuals within the target organization. Most modern governments and corporations are at least partially corrupt. Find evidence of this corruption and use it to compel one or more of these influential individuals to aid your cause. If you are unable to find any evidence of corruption, do not be afraid to bluff. If you make a mysterious window pop up on, say, a CFO's computer that alludes to some sort of dirty secret, it is very possible that the CFO will assume that the hacker who caused the window to appear knows something about them that they actually do not. A lot of powerful people have skeletons in the closet. The media has instilled a fear of hackers into the general populace, and this fear can be used to your advantage. Most normal people, upon being confronted by a hacker that has gained complete control of their computer, will be inclined to believe plausible sounding white lies. Having an "inside man" within your target organization can be extremely useful.

Interlocking Stratagems in Practice

In this section I shall present an example of a plausible situation that could warrant the involvement of hacktivists and a corresponding attack loosely built upon the stratagems from the last section. I have tried to make the situation realistic, but it is very likely that if you use my writing to plan and execute your own attack it will play out nothing like the attack depicted below. Most

actual attacks are far more complex than the one presented here. The purpose of this example is to demonstrate the way in which multiple strike teams should work together. Notice how at all times each team has one or more specific goals.

Situation: A hacktivist collective has decided to attack the terrorist organization Bina Al-ar-mal after they captured and executed a tourist in Syria. Bina Al-ar-mal is believed to consist of over 40,000 people, has hundreds of public Twitter feeds and Facebook accounts, and runs a small terrorist news site hosted on a Russian server. It has three known leaders, who we shall refer to as Head Terrorist 1, Head Terrorist 2, and Head Terrorist 3. Twenty-seven hacktivists have joined the effort. They have been split into three teams: team 1 consists of five of the most highly skilled hacktivists, team 2 consists of seven moderately skilled hacktivists, and team 3 consists of fifteen amateur hacktivists.

Time Line:

(Day 1, Hour 1) Team 1 is initially tasked by the collective with infiltrating as many terrorist Twitter and Facebook accounts as possible. The team starts enumerating the accounts immediately. They decide that no drill will be executed, as breaking into Facebook and Twitter accounts is a trivial task.

(Day 1, Hour 1) Team 2 is initially tasked by the collective with infiltrating the web hosting provider hosting the terrorist group's website. They begin reconnaissance.

(Day 1, Hour 1) Team 3 is initially tasked by the collective with attacking Bina Al-ar-mal's website directly. They begin to map the website.

(Day 1, Hour 2) Team 1 finishes enumerating the terrorist Facebook and Twitter accounts. They begin attempting to break into them.

(Day 1, Hour 2) Team 3 finishes mapping Bina Al-ar-mal's website and begins to attack.

(Day 1, Hour 3) Team 1 has breached a few terrorist Facebook and Twitter accounts. After examining their contents they determine that the terrorists are using SpookyMail email service to communicate off of social media. A few terrorist email accounts are identified and the team begins to try to break into those as well.

(Day 1, Hour 3) Team 3 gains read/write access to a limited portion of the server Bina Al-ar-mal's website is hosted on. The other teams are alerted. They set up a simple php based IP logger script to capture the IP addresses of Bina Al-ar-mal members attempting to check their organization's news feed.

(Day 1, Hour 6) Team 2's reconnaissance ends. They have located the web hosting provider and gathered information on said provider's website and servers. They begin attacking them.

(Day 1, Hour 7) Team 1 breaches their first few terrorist email accounts.

(Day 1, Hour 9) Team 2 locates a vulnerability in the the terrorist's web hosting provider's website. They are not able to fully compromise any of their servers, but they are able to get a list of customer names, domain names, and billing addresses by exploiting a flaw in the website's shopping cart feature. Upon inspecting the list, they discover that the person paying Bina Al-ar-mal's hosting bill has a British billing address. The other teams are alerted and Scotland Yard is notified of the terrorist threat immediately.

(Day 1, Hour 23) Team 1 is able to get Head Terrorist 1's email address off of the "contact" pane of one of the hacked terrorist email accounts. They make ready for a spear phishing attack against him, but decide to wait some time to launch it, as it is currently the middle of the night where Head Terrorist 1 is believed to be.

(Day 2, Hour 3) Team 3 has gathered over seven thousand IP addresses of people viewing Bina Al-ar-mal's news feed and tries to attack them all using known router vulnerabilities. When all is said and done they have infected thirty-seven routers and forty-six workstations. They determine that thirty-four of these work stations belong to active members of Bina Al-ar-mal. They observe these workstations passively, hoping to gather information. The other two teams are briefed on their success.

(Day 2, Hour 8) Team 1 launched a spear phishing attack against Head Terrorist 1 using the hacked email account of another terrorist.

(Day 2, Hour 9) Team 1's spear phishing attack against Head Terrorist 1 is a success. They now have full control over his Windows XP laptop and inform the other two teams of their success. After searching the laptop's hard drive and downloading a half gigabyte of confidential documents and IM logs, the team decides to plant a PDF of the Christian Bible on it along with some real looking fake papers from the CIA. After gleaning Head Terrorist 2's and Head Terrorist 3's email addresses from the stolen IM logs, the team sends them both emails from the hacked email account of a lower level terrorist claiming that Head Terrorist 1 is dirty.

(Day 2, Hour 9) Team 3 decides to take the sensitive information stolen from Head Terrorist 1's computer stolen by Team 1 along with other fake CIA documents and place it on all thirty-four of the terrorist workstations they control. They use a hacked email account belonging to an uninvolved terrorist to inform Head Terrorist 2 and Head Terrorist 3 that Head Terrorist 1 is a traitor and he has at least thirty-four moles inside of their organization, all of whom they mention by name.

(Day 2, Hour 10) Head Terrorist 1's laptop is searched by security forces under the control of Terrorist 2. Head Terrorist 1 is determined to be part of the CIA and is placed into a cell to be used as leverage against the United States.

(Day 2, Hour 17) Head Terrorist 2 and Head Terrorist 3 raid all thirty-four of the suspected moles and find the planted documents. They begin to interrogate

all thirty-four of them in order to find out how deep the CIA has penetrated their organization. None of them know anything but most of them make up real sounding false information to make the interrogations end.

(Day 3, Hour 3) Team 1 determines that most remaining Facebook and Twitter accounts can not be breached. Several team members leave and a few stick around to try and finish off the remaining accounts.

(Day 6, Hour 17) Scotland Yard arrests the person allegedly paying for Bina Al-ar-mal's web hosting. It is later determined that the person is actually part of a London-based Bina Al-ar-mal cell.

(Day 6, hour 20) Team 2 destroys Bina Al-ar-mal's web site after catching word of the Scotland Yard raid.

End Result: One of three head terrorists is being held by their own organization as a traitor and thirty-four unrelated terrorists are being held by their own organization and brutally interrogated about actions they did not commit. One terrorist is in the custody of the Scotland Yard, and a British terror cell has been exposed. Bina Al-ar-mal's entire communication network is compromised (but they do not know that yet), and their website has been taken offline permanently. All members of Bina Al-ar-mal are now becoming increasingly suspicious of their fellow members and the hacktivist collective is now in a position to launch further attacks on Bina Al-ar-mal (using the compromised email and social media accounts) at a later time. This has all been accomplished in under a week.

My public key is available here:

<http://pastebin.com/VhW0bmAt>
<https://paste.ee/p/C5M3U>
<http://tny.cz/c9b82da0>
<http://hastebin.com/jikebijifu.hs>
<http://chopapp.com/#w04dkx06>

SHA1: cb36db996bb684e569663ca7b0d93177ecc561be

Grab it while you still can.

purposes only. The ideas presented here are solely academic and should never be acted upon or put into practice. The author of this document will not be held responsible in the event any criminal or civil charges be brought against any individuals misusing the information in this document to break the law.

-----BEGIN PGP SIGNATURE-----

iQIcBAEBCgAGBQJlUWbobAAoJEDWMWw6MLtALcMgP/3FVybGLvoK2rigce8BoxIVx
lO6UKO0jh8iUpWxSKFC1ml9phCed8Dhx1nb9bwuY6Cwa5NPnn8+R8O98wyvzW5aX
4UVytZ8aqxn83RocLGjkRF6TaCBFaD3V81IHaNy1ODuXBGVR7IG4djS6pDw9BJda
f19L3a8zdr8yoczisdpcklWEqWfLSRgwkOcJ9xtDYG6FuDjs++4ZdncUfwCg76aw
xYJVACdXsl1VDjVtGr1Fx756DuPkFr5APQG64dor5iOxhXw+9sEVD7AnzjpSCxCK
MtaHzkuiwnp38z9PlaSPqxwyNZ6t8F9FPsgf76x7+egqZO/Q158NR7gGb1XqaL9
V6mopDiGeQveHePG1zpOv22YBMkrxi0KjFDDTOM/xYBw/+wZnjXjoL+eC2vegQxU
cvcntSXN8l5Wtjc+mX9GdKF+RmjQvN62TmPxB9i35ZhdR7ogk1uqPGqxbova6v/f
3VSfroFWoOo2wkx/aZLpo3Sqe6JS+IRBpZkysWsJHcbNjUfYG6BDWameXvBulecB
Q1kdRhrQKayoaVOVrzLTmm4T+Nu9/OVcdx9AO5FF4eShHNa93ybDVOcUaweYoO/K
CngW+eRkz2B+YOOToeAq9JfvAlo89HUWCRj+OOvWsjJAy5eEQWYch2X7b7CyGkZb
U4SaSVZVhGFN1kQgCIIV
=QuZa

-----END PGP SIGNATURE-----